A Brief Overview of Sandia National Laboratories – IO/IA Modeling Research & Development

Bob Pollock

Infrastructure & Information Technology Department

Sandia National Laboratories

(505) 844-4442 rdpollo@sandia.Gov

September 06, 2001

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy under contract DE-AC04-94AL85000.

Sandia National Laboratories

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	9/6/2001	Report 9/6/2001

4. TITLE AND SUBTITLE
A Brief Overview of Sandia National A Brief Overview of Sandia National Laboratories IO/ IA Modeling Research & Development

5. FUNDING NUMBERS

6. AUTHOR(S)
Bob Pollock

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Sandia National Laboratories
Infrastructure and
Information Technology
Department

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

An overview of Sandia National Laboratories contribution to IO/IA Modeling and Research.

14. SUBJECT TERMS
IATAC Collection, information security, cryptography, information assurance, threats, intrusion detection

15. NUMBER OF PAGES
55

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	abstract_limitation

NSN 7540-01-280-5500

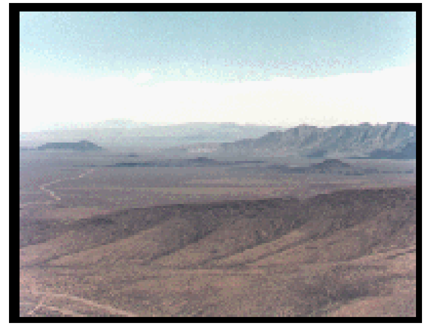
Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

What Is Sandia

- **National security laboratory**
- **Our Primary mission is nuclear weapons**
  - **responsible for more than 95% of weapon components**
- **Nearly 1/4 of our work supports DoD and intelligence community**
- **Broader mission in science and engineering to meet national needs**

Sandia Is Distributed Across Many Sites

Albuquerque, New Mexico



Yucca Mountain

WIPP, New Mexico

Livermore,California

Tonopah Test Range
Nevada

Kauai Test Facility
Hawaii

Sandia–in Round Numbers

- **7,500 full-time employees**
  - ~6,600 in New Mexico
  - ~900 in California
- **700 buildings, 6M sq. ft.**
- **1,400 Ph.D.'s, 2,100 Masters**
  - 54% engineering
  - 24% science and mathematics
  - 22% computing and other
- **Annual budget $1400M**

Infrastructure and Information Systems Engineering Center (6500)

Organization

Sam Varnado, Director

Ron Trellue, Deputy Director
Technology Development

Larry Ellis, Deputy Director
Strategic Development

Business Area Domains

Satellite-based sensor information systems.

Decision support systems for distributed and other Environments.

Information assurance and survivability for national security systems.

Project/Technology Domains

Mission/Solution Engineering

- Life-cycle SW Engineering
- Decision Support Systems
- High-integrity real-time software systems
- Critical infrastructure protection
- Information assurance solutions for DOE, DoD, and other agencies
- Secure Ad-Hoc Wireless Systems

Domains

- Architectures & Frameworks
- Real-time Systems
- Event/Signal Processing
- Distributed Environments
- Modeling & Simulation
- Knowledge Generation
- Information Security
- IT Assessments

Technologies

- OODB
- XML
- CORBA, RMI
- Java, C++
- Intelligent Agents
- GIS
- Web Apps

IA/IO Modeling & Simulations

Communications modeling

- Vulnerabilities in Wireless Ad Hoc Networks
- Simulations of Wireless Ad Hoc Networks
- IA Overhead in Wireless Ad Hoc Networks
- IA for wireless ad-hoc networks (With robots in urban conflict environments)
- Network devices

Critical infrastructure simulation

- Agent-based micro simulation (ASPEN modeling tool)
- NISAC program
- SCADA testbed simulations

Cryptographic research

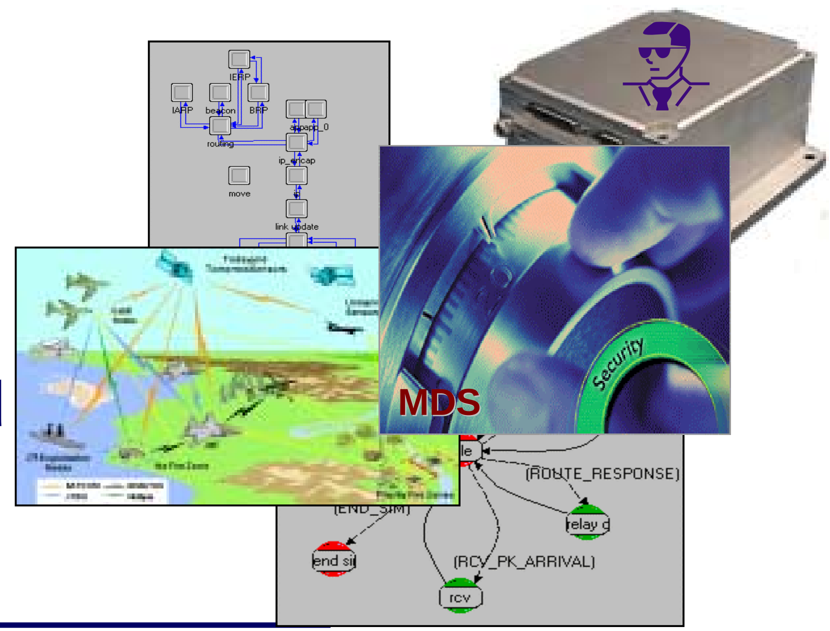
- Efficient, low power signature algorithms
- Secure, wireless communications
- Proactive, threshold cryptography
- Surety for SCADA systems
- Anonymous, authenticated communications

Analysis tools

- Graphic-based network vulnerability
- Modeling behavior of the cyber-terrorist

Communications Research

- Vulnerabilities in Wireless Ad Hoc Networks
- Simulations of Wireless Ad Hoc Networks
- IA Overhead in Wireless Ad Hoc Networks
- Network Devices



Systems Approach to the Wireless Communications Environment

Wireless Environment

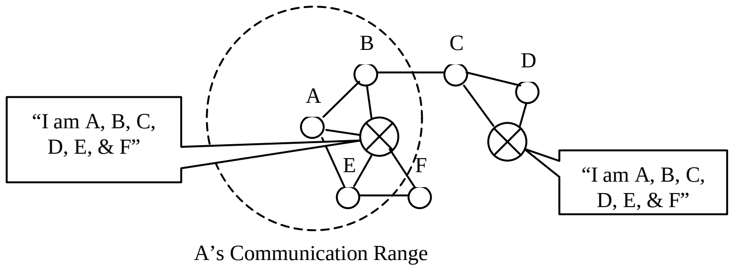
- **Resource Constraints**
  - RF Bandwidth
  - CPU Limitations
  - Battery Size
- **RF Stressors & Issues**
  - Environmental Interference
  - Terrain Interference
  - Adversarial Interference
  - Covertness; LPI/LPD
  - Antenna Placement
- **Network**
  - Dynamic Topology & Mobility
  - Scalability, Performance

IA Technologies

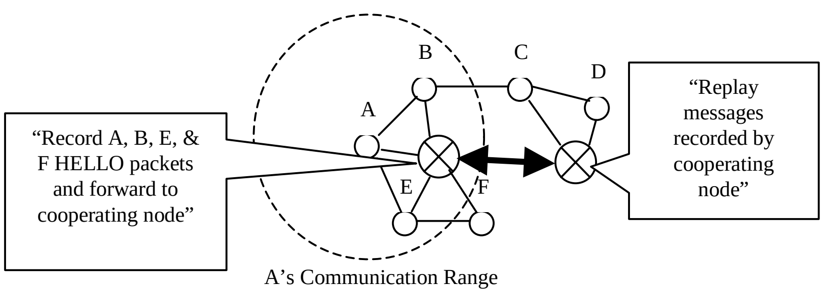
- **Cryptography**
  - Low-Power Approaches
  - Threshold
- **Non-Cryptography**
  - Redundant Routes
  - Source Initiated Route Switching
  - Onion Routing
  - Encapsulation
  - Sequence Numbers/Time Stamp
  - Intrusion Detection

Vulnerabilities in Wireless Ad Hoc Networks

Research of Vulnerabilities in Wireless Ad Hoc Networks



⊗ Adversary Node



Objective:

Identify vulnerabilities in wireless ad hoc networks that adversaries can exploit to reduce or eliminate effectiveness of network.

Relevance:

Vulnerabilities and exploits must be clearly identified to develop IA techniques and approaches.

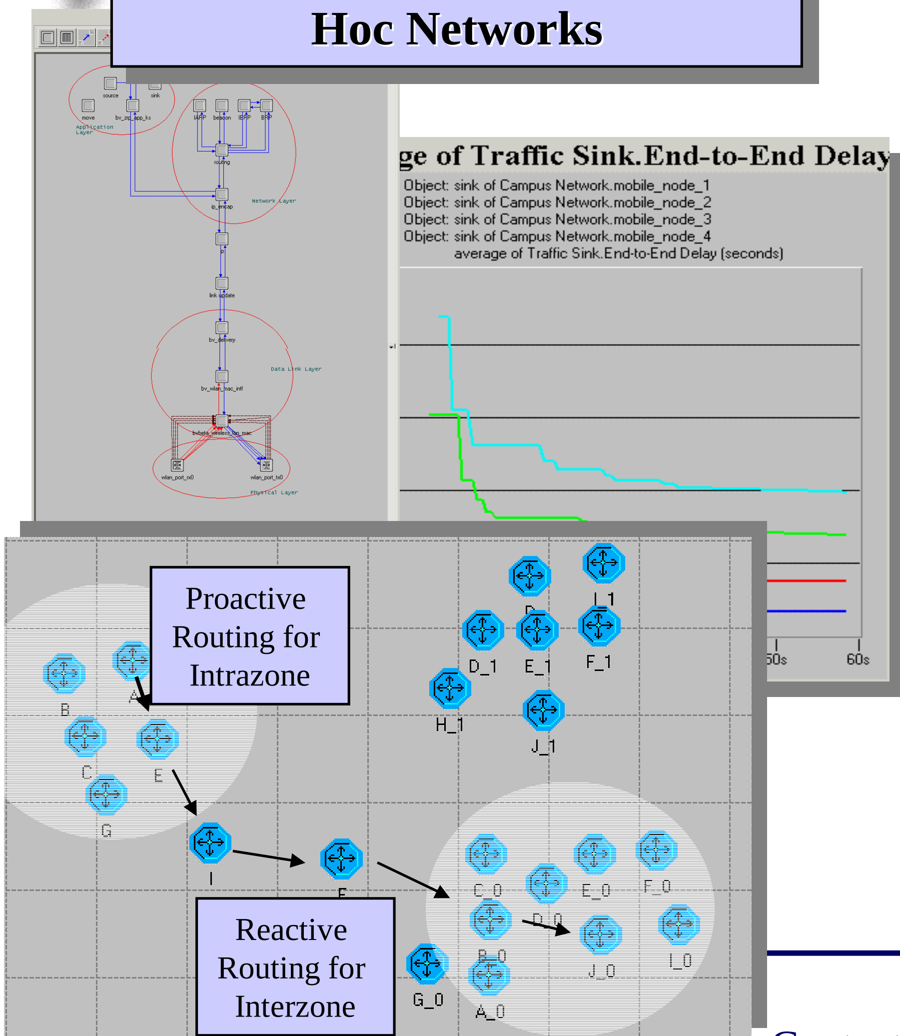
Status:

Network vulnerabilities and techniques to exploit have been identified and described in a report.

Contact: Brian Van Leeuwen, bpvanle@sandia.gov

Simulations of Wireless Ad Hoc Networks

Stimulations of Wireless Ad Hoc Networks



Objective:

Develop simulations to evaluate the performance and practicality of mobile wireless protocols.

Relevance:

Various routing and MAC protocols have been proposed and their performance must be evaluated for their effectiveness before implementation into systems.

Status:

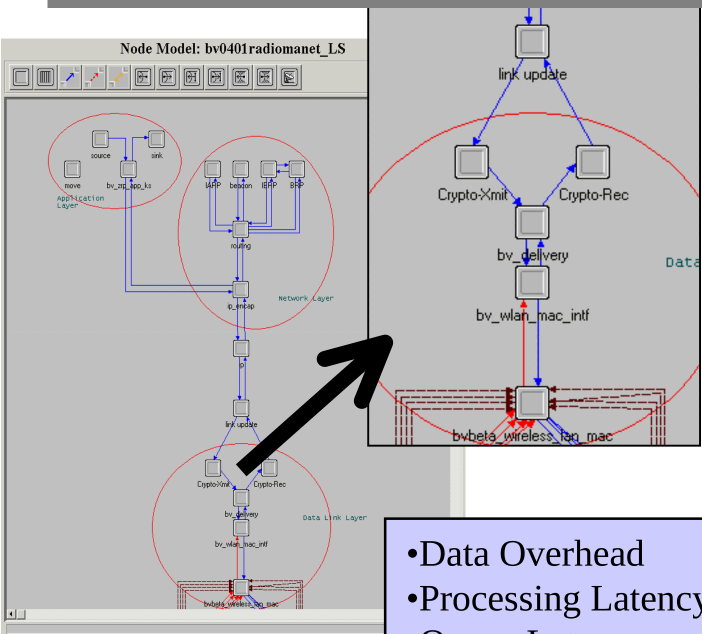
Implemented model of the Zone Routing Protocol in OPNET to evaluate performance issues such as: scalability, control overhead, and network convergence.

- With and without high-fidelity representation of MAC layer protocol
- With and without cryptographic overheads

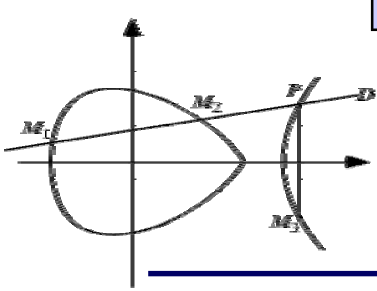
Contact: Brian Van Leeuwen, bpvanle@sandia.gov

IA Overhead In Wireless Ad Hoc Networks

Research of IA Overhead in Wireless Ad Hoc Networks



- Data Overhead
- Processing Latency
- Queue Latency



$$y = \sqrt{x^3 + ax + b}$$

Objective:

Identify overhead impacts of cryptographic security approaches in mobile wireless ad hoc networks.

Relevance:

Cryptography consumes significant node and network resources. In resource constrained wireless systems these overheads will degrade network performance.

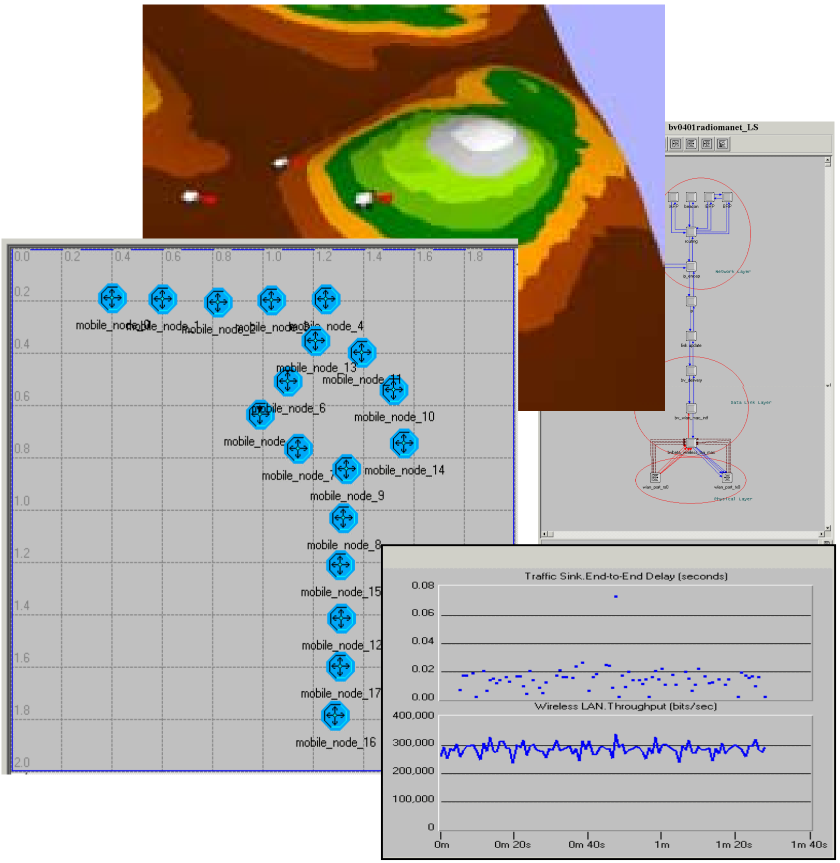
Status:

Simulations are being executed and data is being collected.

Contact: Brian Van Leeuwen, bpvanle@sandia.gov

Environment Effects

Terrain and Environmental Effects on Wireless Information Assurance



Objective:

Enhance system simulations by incorporating the effects of environment on mobile wireless communications. This will be done by integrating statistical error allocation into the communication simulations with Sandia's Umbra system level simulator.

Relevance:

Accurate modeling of terrain and other environmental stressors will improve information assurance (IA) design in wireless communication systems. Improved wireless IA design will enhance overall performance of fielded systems.

Status:

Activities begin in October, 2001

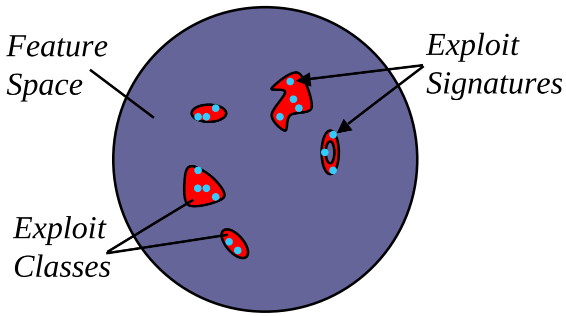
Control Plan Security for Wireless/wired Gateway

Goal: To minimize the impact of security protocols while maintaining the security robustness at the transition between wired and wireless networks.

Approach: The interaction between security protocols at the wired/wireless interface will be investigated for vulnerabilities, which will guide modifications to the security protocols and system configurations to reduce the security risk at the interfaces.

Contact: Brian Van Leeuwen, bpvanle@sandia.gov

Generalized Signature-based Intrusion Detection using Adaptive Critic Designs



Generalized Signature-Based Intrusion Detection

GOAL:

Develop techniques to detect novel attacks/exploits.

PROBLEM:

- Novel attacks are hard to detect.
- Signature-based ID is too narrow - can't detect new exploits.
  High incidence of Type I events
- Anomaly detection is too broad - detects too many anomalies, many of which aren't exploits.
  High incidence of Type II events

OBJECTIVE/APPROACH:

- Generalized Signature-based ID
- Start with known exploit signatures and "grow" exploit classes.
- Train an ID to learn boundaries of exploit classes.
- Able to detect novel exploits that are similar to known exploits.
- Use Adaptive Critic Designs (ACDs) for generalized signature-based intrusion detection.

Contact: Tim Draelos, tjdrael@sandia.gov

Critical Infrastructure Simulation

- Agent-based Micro Simulation (ASPEN Modeling Tool)
- NISAC
- SCADA Test bed

The Nation's Infrastructure Faces a Broad Spectrum of Threats

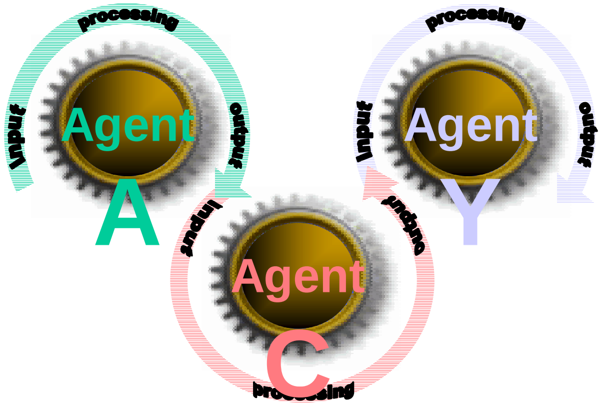
- **Physical Threats**
  - Terrorists
  - Aging and degradation
  - Natural disasters
- **Cyber Threats**
  - Malicious intrusion
  - Inadvertent error
  - Insider Threat
- **System Complexity**
  - Increasing number of interconnections and automation
  - Cascading effects
  - Increasing interdependencies
  - Electric industry restructuring

Photograph by Jim Argo; ©1995, The Oklahoma Publishing Company

How can complex infrastructure systems be analyzed?

Microanalytic Modeling

- **A conceptual shift from a mathematical description of an entire system to specification of the behavior of individual agents.**
- **Agents make real life decisions. Non-linear effects are explicitly treated.**
- **Agents employ evolutionary learning models which are focused on optimizing utility.**



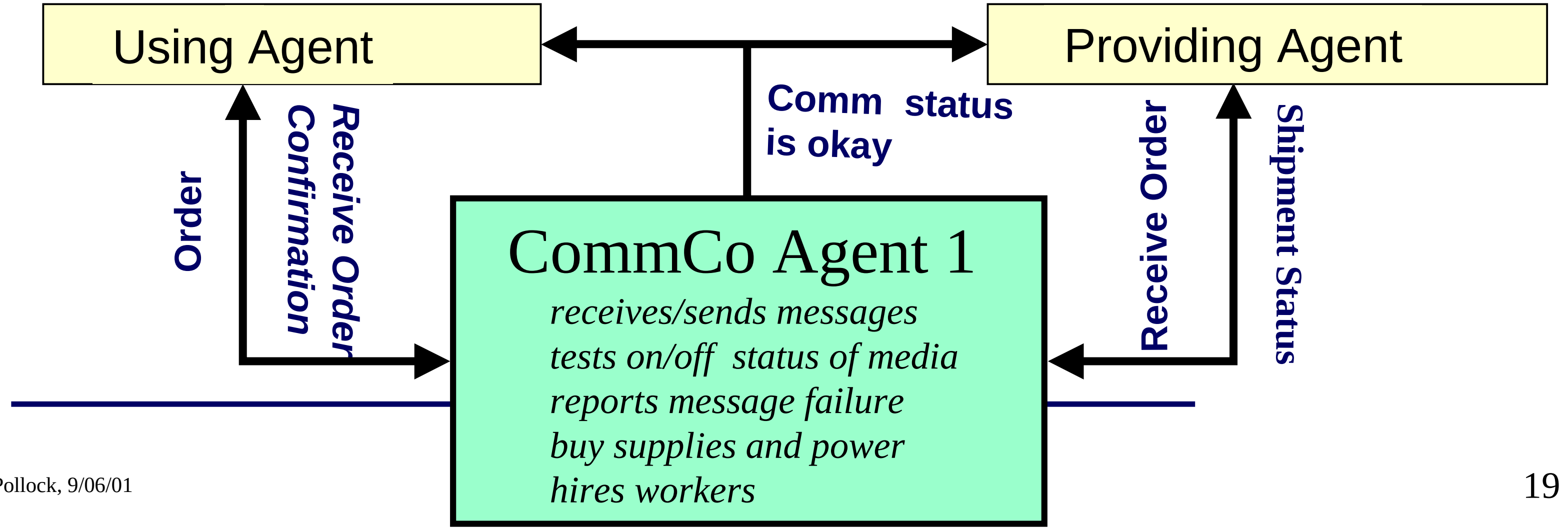
Contact: Dianne Barton, dcmaroz@sandia.gov

We have the ability to quickly develop new agents or draw upon our current library of agent types and modeling expertise to build exactly the simulation that a customer requests

CommASPEN

An agent based model that simulates the role of telecommunication on critical infrastructure interdependencies

- **Communication agents (CommCo Agent) are generalized suppliers of communication service in the model.**
- **The model simulates how telecommunication infrastructure affects the exchange of information and services between agents and the dependence of telecommunication on sectors like power.**



NISAC Program

A partnership between LANL and SNL that will leverage existing research and development activities to support industry and government agencies in protecting the critical infrastructure to enhance national security.

MISSION: to improve the nation's security and the robustness of the nation's infrastructure by establishing a state-of-the-art modeling and simulation environment that will:

- Provide the most advanced analysis expertise for understanding infrastructure interdependencies, vulnerabilities, and system complexities;
- Determine the consequences of infrastructure outages; And.
- Optimize protection and mitigation strategies.

Contact: Jennifer Nelson, jenelso@sandia.gov

Potential Users & Applications of NISAC

Private Industry

Infrastructure Vulnerability Analysis & Mitigation Trade-offs

National Security

- DTRA
- CINCS
- JPO
- Intel Community

Planning, Protection &Training

Federal, State & Local Government Agencies

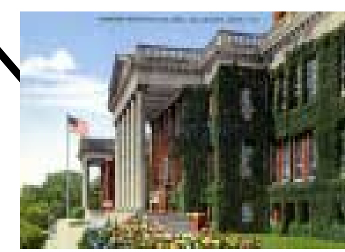
- FEMA
- National Guard
- DoJ
- DOE

Government Policy Analysis

Emergency Response Contingency Planning

Consequence Mitigation & Management

Universities



Education

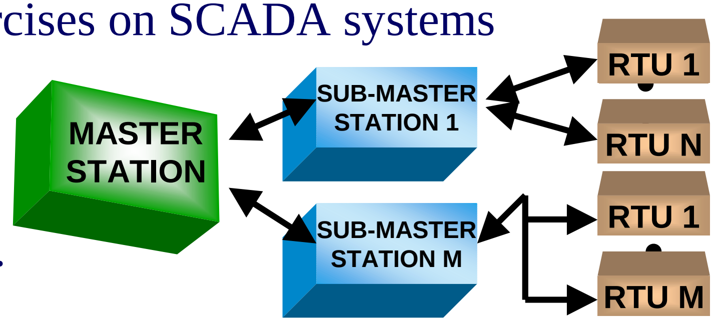
Secure SCADA Development Lab

PROBLEM:

- Supervisory control and data acquisition (SCADA) systems are used to control many critical infrastructures.
- Historically, security has not been included in SCADA components or architectures.
- A facility is needed to analyze SCADA security and to test and validate new SCADA security concepts.

OBJECTIVE/APPROACH:

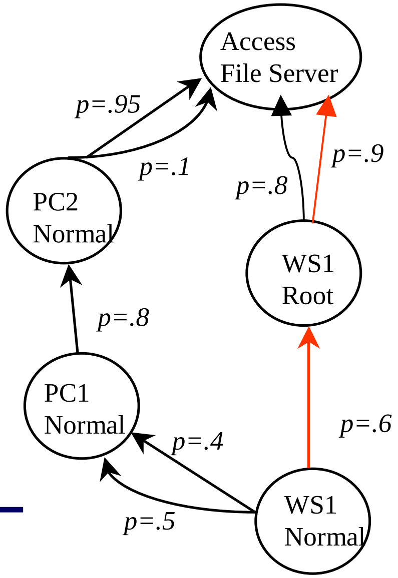
- Develop a testbed with representative elements of a SCADA system.
- Perform vulnerability assessments and security exercises on SCADA systems and hardware/software components.
- Develop new security concepts and methodologies.
- Model and simulate operational SCADA systems.
- Educate stakeholders about SCADA security issues.



Contact: Juan Torres, jjtorre@sandia.gov

Modeling Tools

- Modeling Behavior of the Cyber-terrorist
- Graph-based Network Vulnerability



How do we model adversaries to an information system?

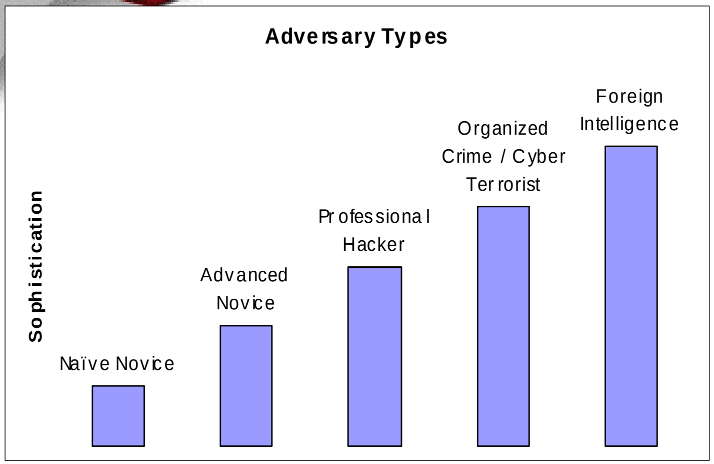
Variables in our models include:

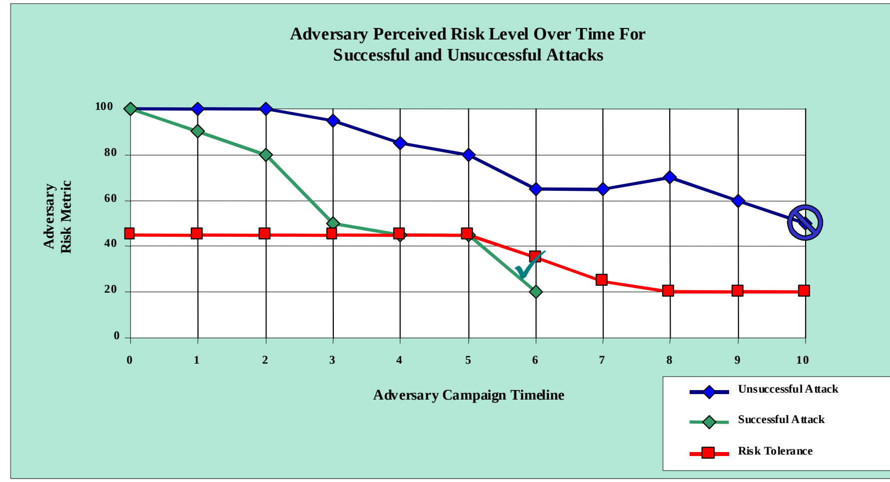
- **Sophistication -** Hacker, terrorist, nation state, foreign intelligence… ?
  A terrorist organization or small nation state

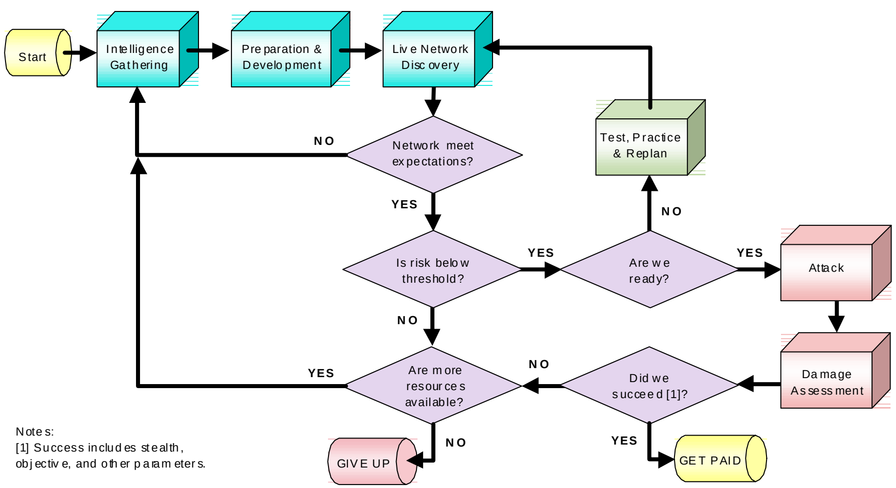
- **Resources -** Money & “magical powers”
  Well funded can afford skills and assistance to learn all design information
- **Mission -** What is the adversary’s overall goal?
  Has specific goals & objectives generally to limit effectiveness of a critical info system.
- **Risk Tolerance -** How hard does the adversary avoid detection?
  Risk averse, but very creative & very clever…

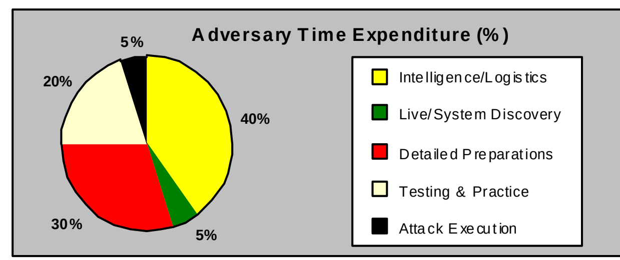
Most common adversary model: Cyber-terrorist

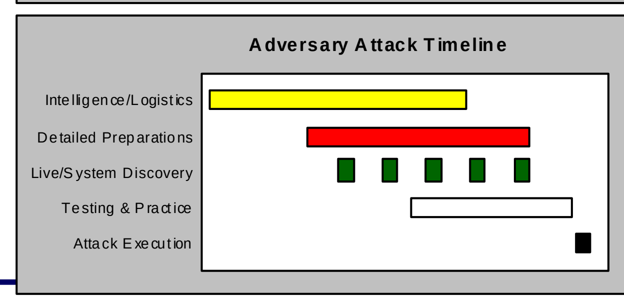
Cyber-terrorist Model











Graph Based Network Vulnerability

- ***GOAL***: To provide a state-of-the art tool which will perform a quantitative analysis of computer networks
  - Identify sets of exploitable vulnerabilities
  - Means to compare deployed and proposed architectures
    - Examine configuration options and new equipment integration
    - Policy issues for a given mission/network system
  - Suggest optimal defense placement and response options
    - Determine attack path defeat (blocking)
  - Use formal methods to enumerate network threats and attack paths

Contact: Dave Ellis, dellis@sandia.gov

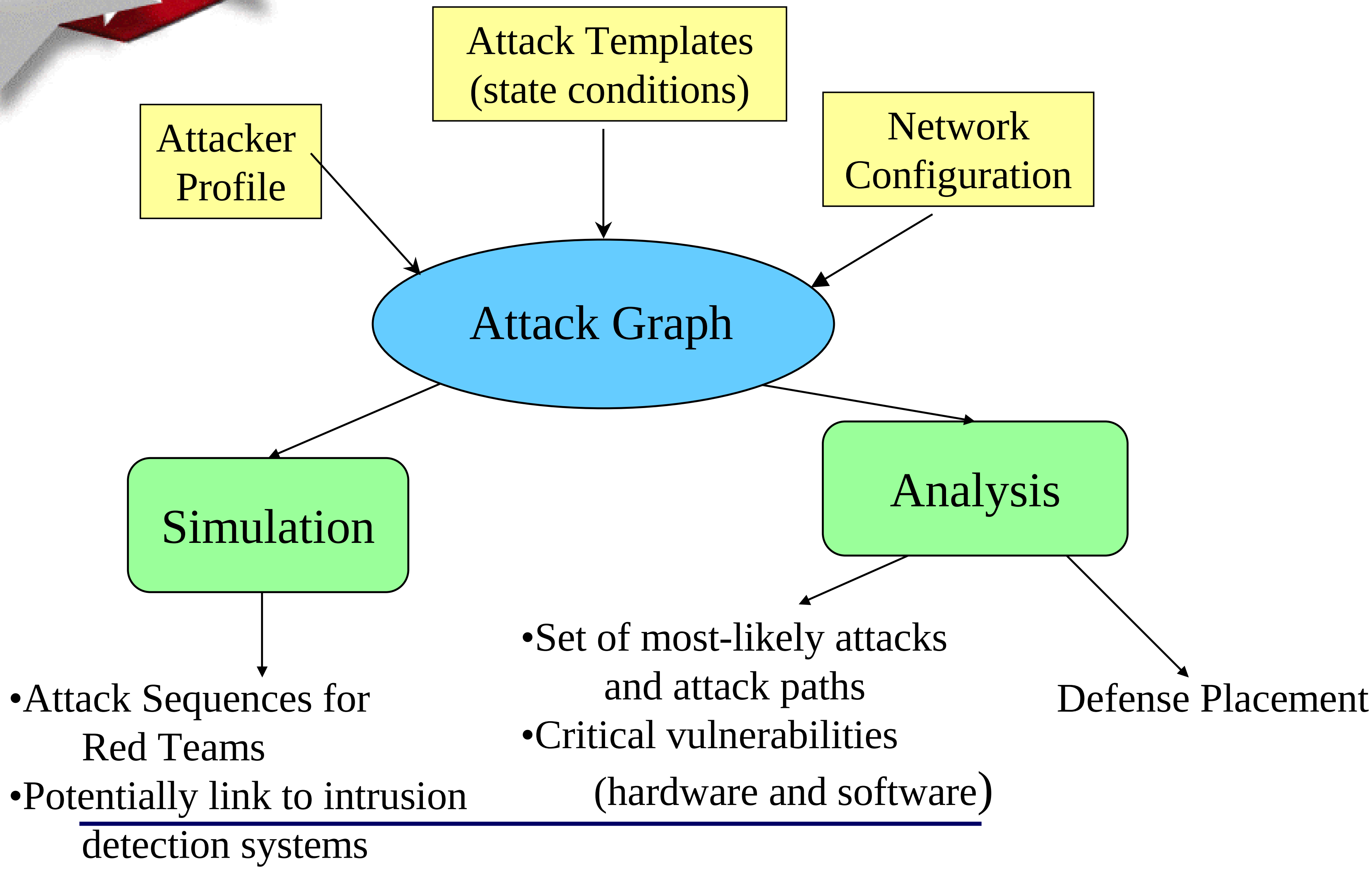
Why This Research Is Important

- Identify likely list of paths to attack a goal or list of paths from an entry point
- Identify the most critical nodes and edges for a given set of metrics and attacks
- Evaluate the cost/benefit in network design
- Suggest the most cost-effective defense placement
- Evaluate security metrics
  (e.g., time to attack, probability of detection)

Customers

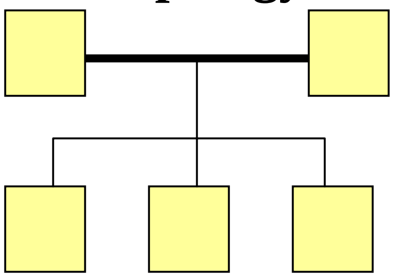
- DARPA Information Assurance Science and Engineering Tools Program (IASET)
- Other government agency

Attack Graph Concept

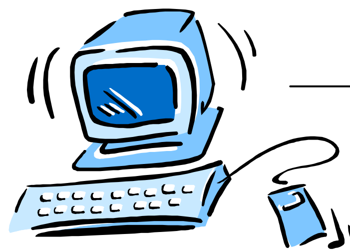


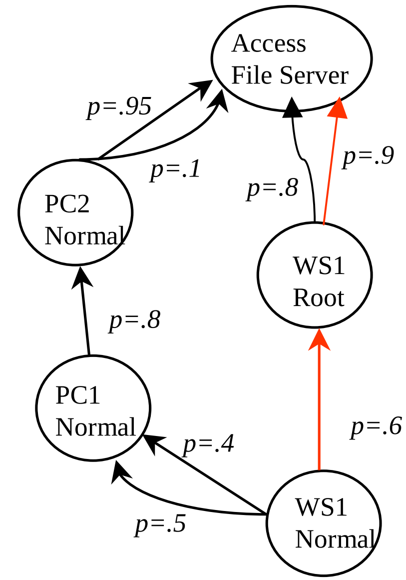
Attack Graph

Network Topology/Configuration



Graph Generator





Sources of Exploits
- experts
- commercial tools
- non commercial tools

Risk Metrics
- Cost/Effort
- Prob. Of Success
- Prob. Of Detection
- Time
- etc.

List of Exploits

– Innd mailbug
– rlogin subvert
– suid_eject
– trojan A
– anon_ftp C
– install sniffer
– NTGetAdmin
– etc.

Attack Graph

- Identify set of most likely attack paths
- Identify most critical nodes and edges
- Suggest cost-effect defense placement
- Use as a testbed for evaluating metrics
- Suggest red-team attack sequences
- Link to intrusion detection systems

Exploits → **Ordered Attacks**

New Capabilities

- **Identify** most significant attack paths **based on user-defined criteria (e.g., Attacker's cost, probability of success, latency)**
- **Identify** critical combinations **of known attacks which highlight possible exploitable vulnerabilities**
- **Model attacks with more granularity and realism:**
  - **Account for learning behavior and different types of attackers**
  - **Model dynamic aspects of network (reconfiguration on the fly)**
- **Defense placement algorithms:**
  - **Develop methods to determine optimal ways to increase shortest paths where multiple edge weights can be increased by a single action. This will allow one to determine the defense placement actions with the highest benefit.**
- **Complex display/visualization tools**

Comparison to Existing Tools

- Analysis and Configuration tools
  - **Check list of services or conditions on each machine on a network**
    (e.g. Internet Security Systems' Scanners, Microsoft's SMS)
  - **Don't consider the network as a whole, how vulnerabilities on individual machines can be leveraged in a full attack**
  - **Our tool uses information from configuration management tools and scanning tools as input**
- Intrusion Detection Systems
  - **Look for specific "signatures" or patterns indicating likely attack**
  - **Our system would be complementary, generating an attack graph forward from suspected security violation, suggesting detector placement.**

Why this research is hard

- Potential set of attack methods is very large
- Need to identify what requirements (e.g., OS type, processes running, privilege level, etc.) are necessary for various attacks and if those requirements are present on the network and where
- Huge number of “matching” operations to match attack templates against network configuration ➨ combinatorial explosion of the attack graph
- Need to find algorithms and heuristics to correctly and efficiently prune the graph

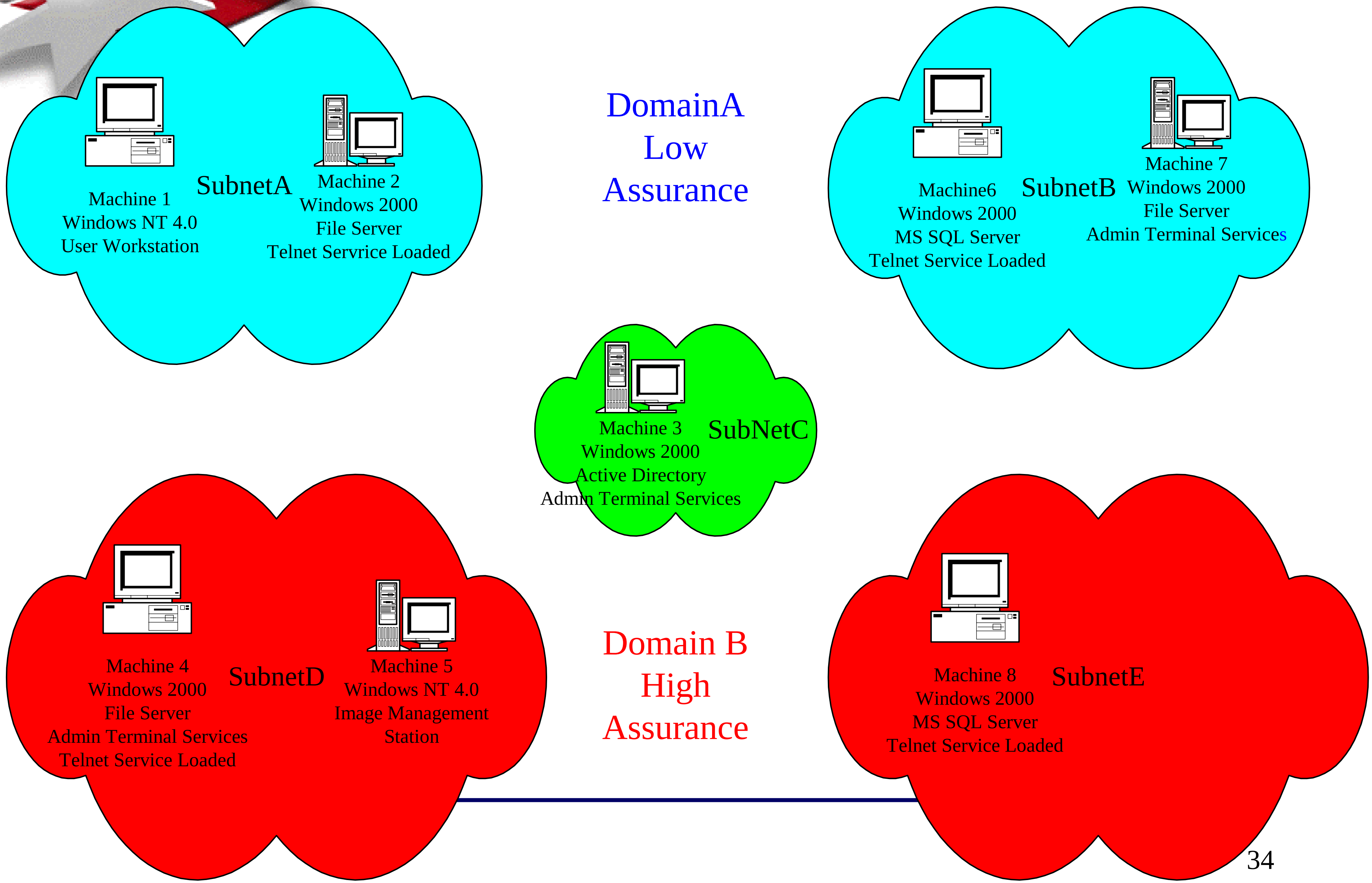
BASIS FOR CONFIDENCE

- We have demonstrated graph generation on a small scale, have developed pruning algorithms, and have pulled real network information from databases to populate the graph

DEMO

- **The next set of slides will walk you through screen shots of our tool, including the following steps:**
  - **Entering attack template information**
  - **Generating machine configuration data**
  - **Specifying parameters for the graph generation and running it**
  - **Viewing the attack graph**

Insider Testbed Simulator



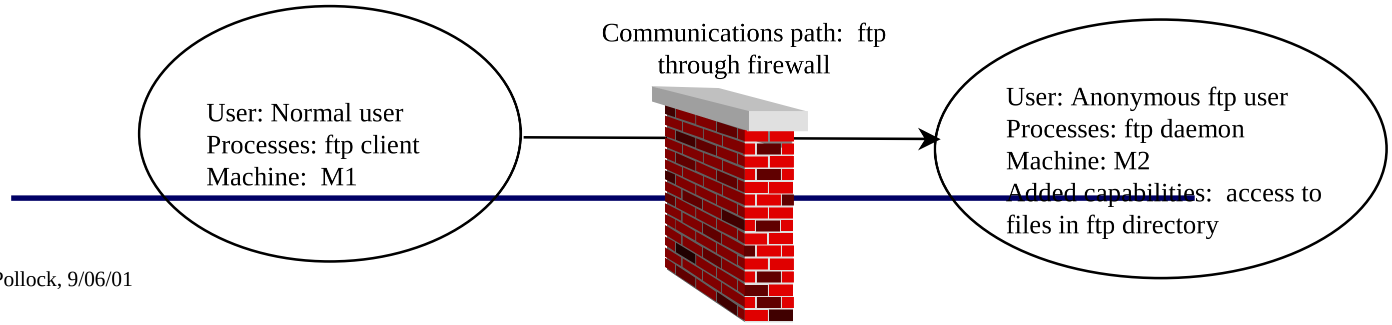
Insider Testbed Simulator

- Modeling an insider attack from a low assurance domain to a high assurance domain
  - Eight machines, 5 subnets, 3 domains
  - Twenty attack templates
- Basic attack sequence involves:
  - Capturing domain accounts on local machine
  - Using domain accounts to activate remote services
  - Using services to obtain remote access and/or command execution (e.g. NFS, windows file sharing, telnet, terminal services)
  - Escalating privileges
  - Repeating above steps
  - And finally read/write data on a target machine

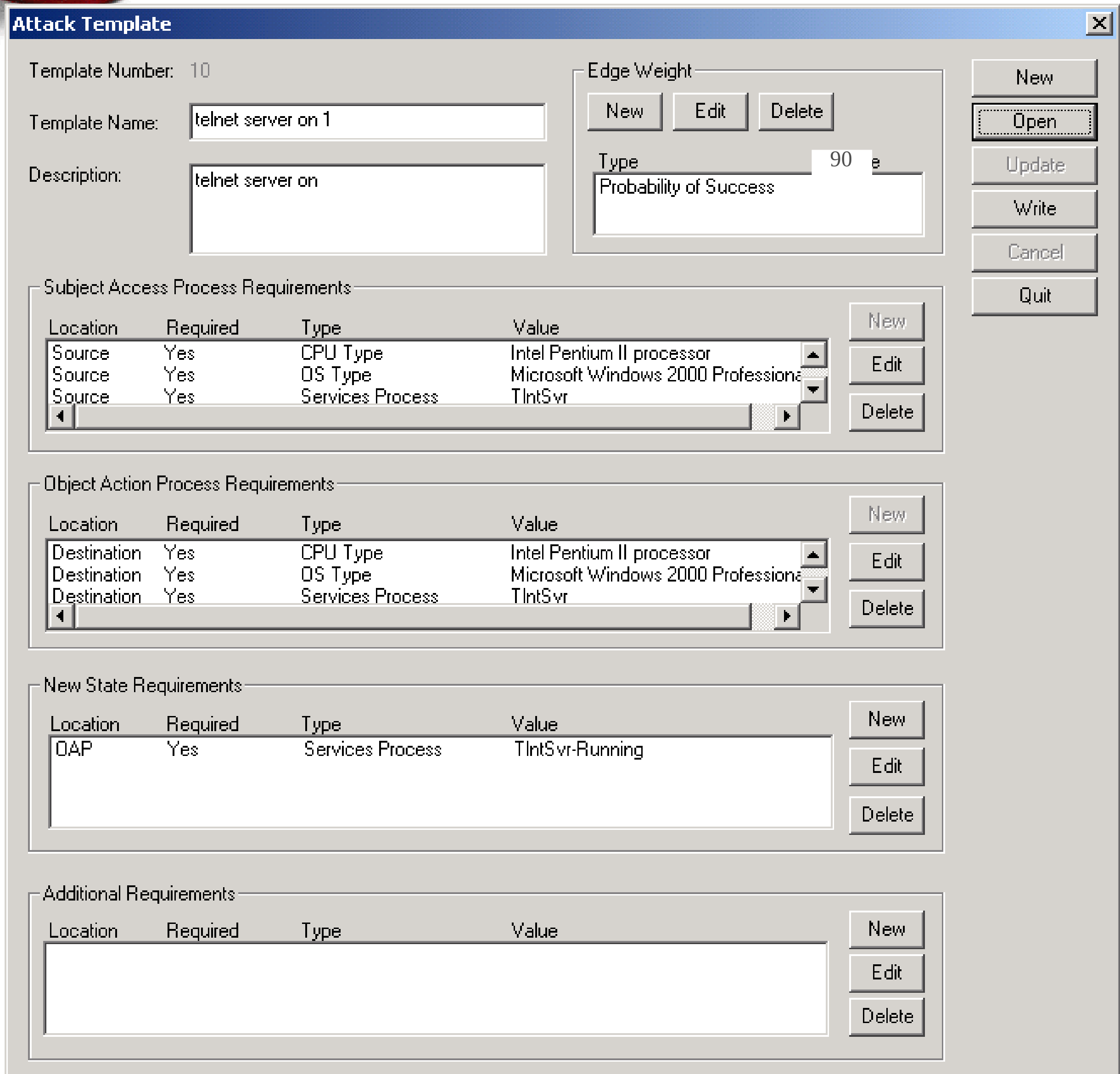
Attack Template

- Contains information about state transitions in known or hypothesized attacks steps
- Template contains:
  - representation of subject application and object action process
  - list of requirements or conditions that must be satisfied for state transition to occur (note: we are adding the capability for arbitrary logic: requirement 1 AND (requirement 2 OR requirement 3)
  - list of vulnerabilities or capabilities created or exposed as a result of the state transition (e.g. reading files without proper authorization, planting a trojan horse, etc.)
  - communications path
  - edge weight (consequence metric of interest)

FTP Template

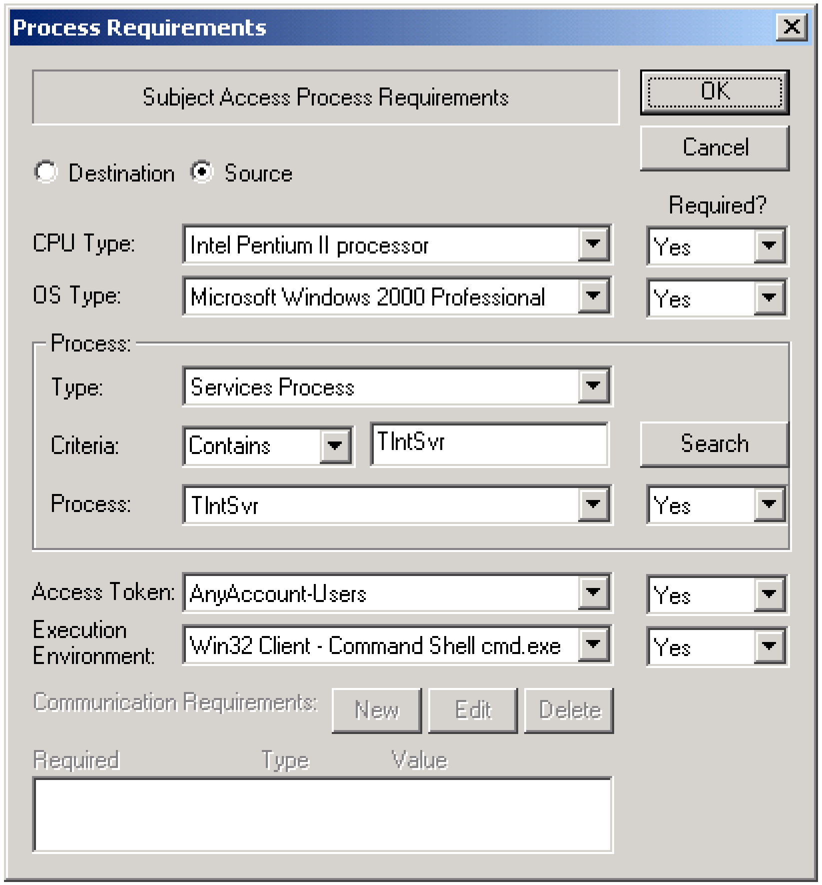


Attack Template Creation



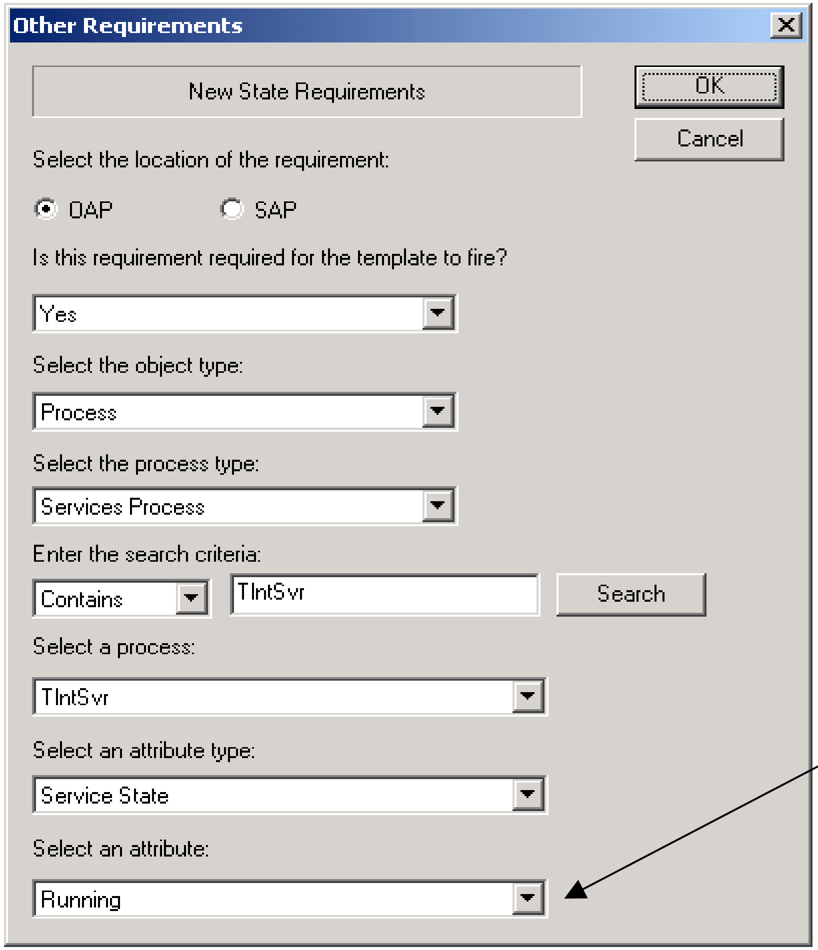
This is the main form for creating attack templates. The user specifies items such as the template name, description, edge weight type and value, then goes to other forms to enter specific requirements for the subject and object processes.

Attack Template Creation



This form allows the user to specify various requirements on how the attacker starts a process, including the CPU type and OS type of the source machine, the process name, the privilege level the attacker is using (denoted by access token), and the execution environment in which the service or process is running.

Attack Template Creation



This form allows the user to specify the "new state", that is the state on the attack destination machine that occurs after the attack has occurred. In this example, the attacker turns on a telnet server on the destination machine.

Example Attack Template File

Template ftp logon

Requirements:

(cpu = "Intel Pentium II processor",SRC)

(ostype = "Microsoft Windows 2000 Professional",SRC)

("Service-FTPServer",SRC)

(SAP-PAT="AnyAccount-Users",SRC)

("ObjectEnvironment-Win32 Client",SRC)

(cpu = "Intel Pentium II processor",DEST)

(ostype = "Microsoft Windows 2000 Professional",DEST)

("Service-FTPServer",DEST)

(OAP-PAT="AnyAccount-BackupOperators",DEST)

("ObjectEnvironment-Win32 Client",DEST)

AddedVulnerabilities:

("Write-FileName",DEST)

Label: ftp logon

EdgeWt: .3

Example Machine File

Machine 240

OS {type "Microsoft Windows NT Workstation"}

OS {rel "Service Pack 6, 4.0.1381"}

CPU {“Intel Pentium II Processor”}

VULN {"Domain = CSU821"}

VULN {"Primary-User = SYSTEM"}

VULN {"Service-Alerter-Stopped"}

VULN {"Service-Alerter-LocalSystem"}

VULN {"Service-Browser-Running"}

VULN {"Service-Browser-LocalSystem"}

…

VULN {"Application-OUTLOOK.EXE"}

VULN {"Application-OUTLOOK.TXT"}

VULN {"Application-OUTLSPEC.INI"}

VULN {"Application-OUTSIDER.EXE"}

VULN {"Application-packager.exe"}

VULN {"Application-PageKeep.exe"}

VULN {"Application-pax.exe"}

VULN {"Application-pbrush.exe"}

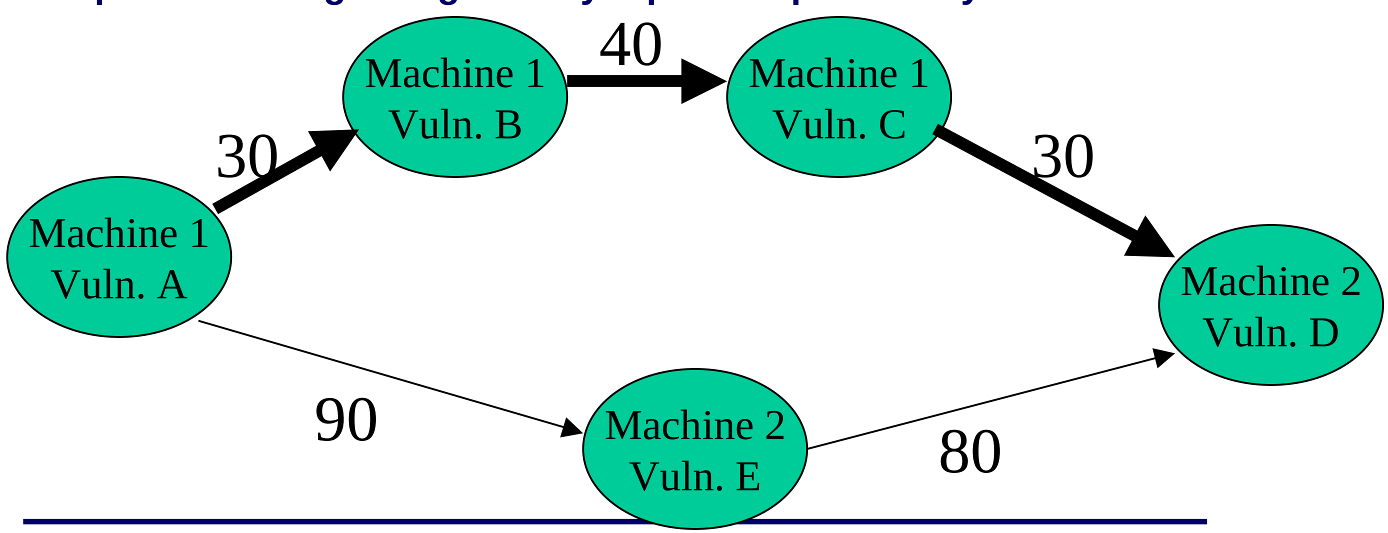
VULN {"Application-pc.ini"}

VULN {"Application-PERFMON.EXE"}

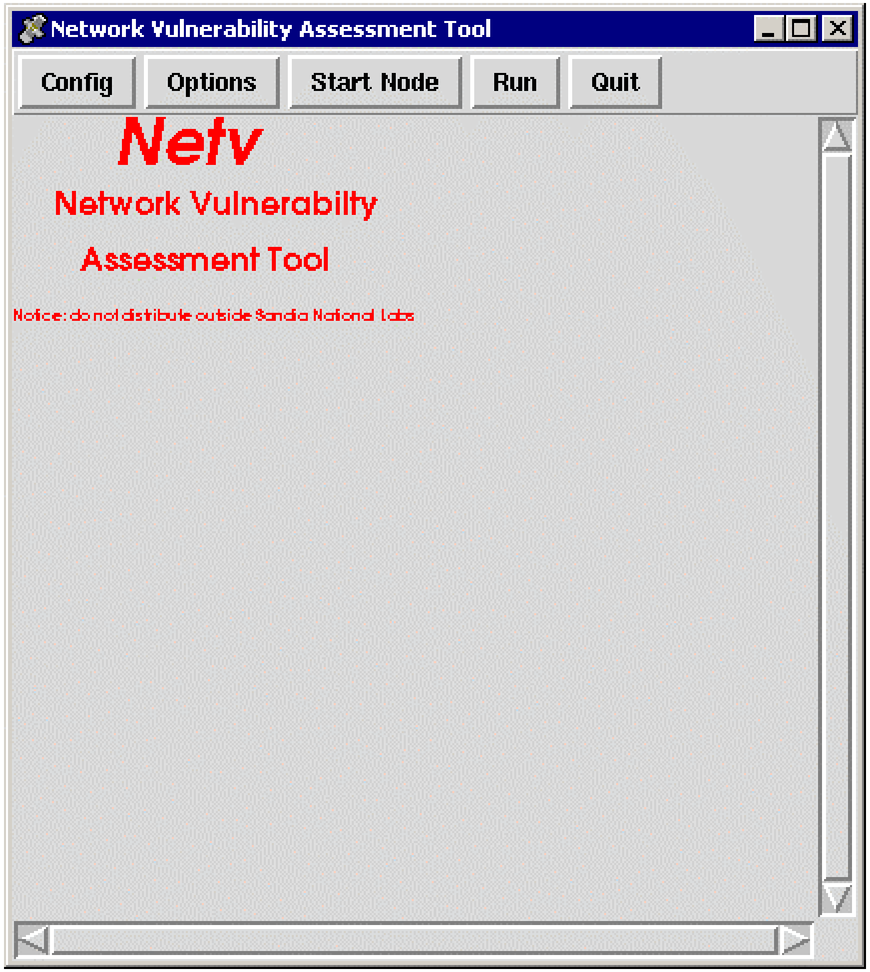
The machine files include information gathered by Microsoft’s SMS system, including OS type and release, CPU type, domain names, and service and application files.

Graph Analysis

- Single shortest path not a good security measure since edge weights are approximations
- Set of all near-optimal paths is better reflection of total system security
  - more robust
  - set of edges on many near-optimal paths together represent most vulnerable points
  - still efficiently computable (Naor, Brutlag '93 for directed graphs)
- Shortest path may not be the one with the fewest steps. As shown below, the highlighted path is shorter, though it involves three steps compared to two steps on the lower path. The edge weights may represent probability of detection or attacker cost.

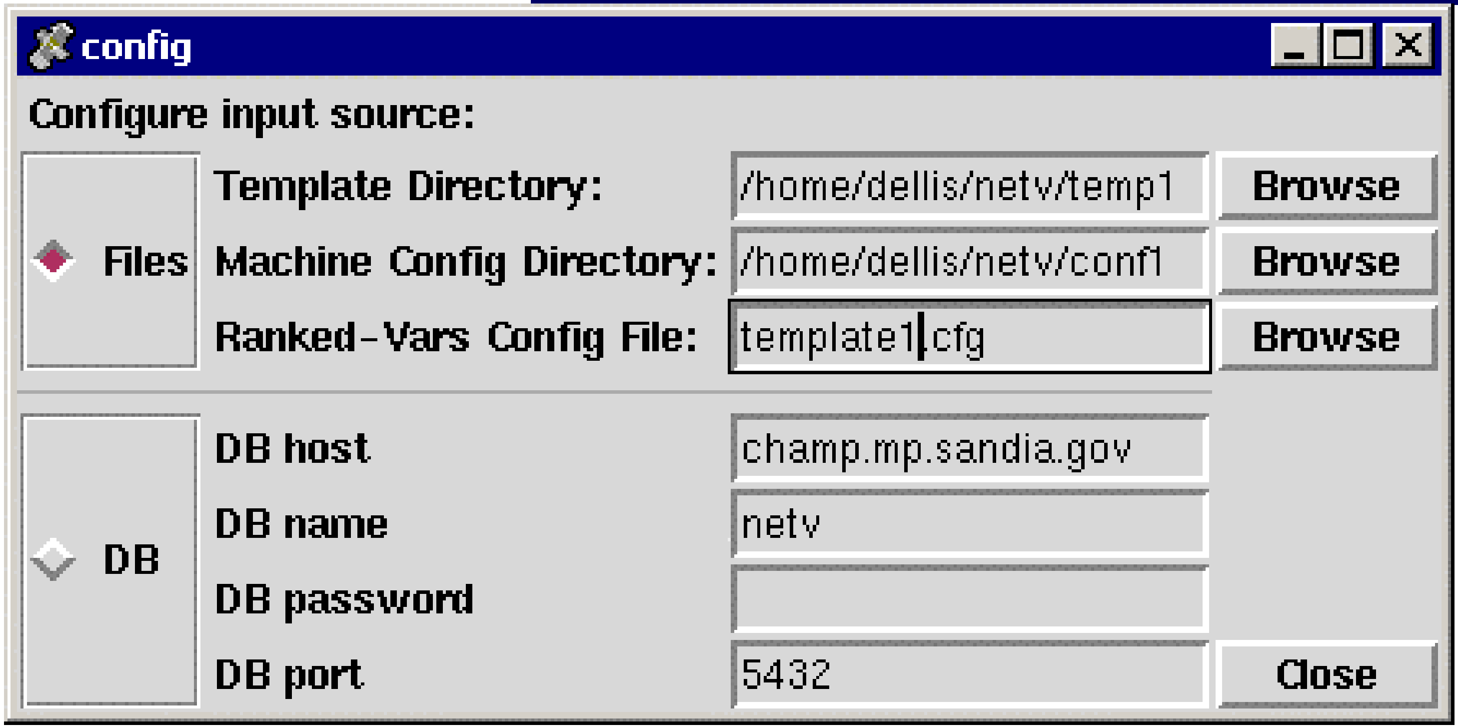


Graph Generator



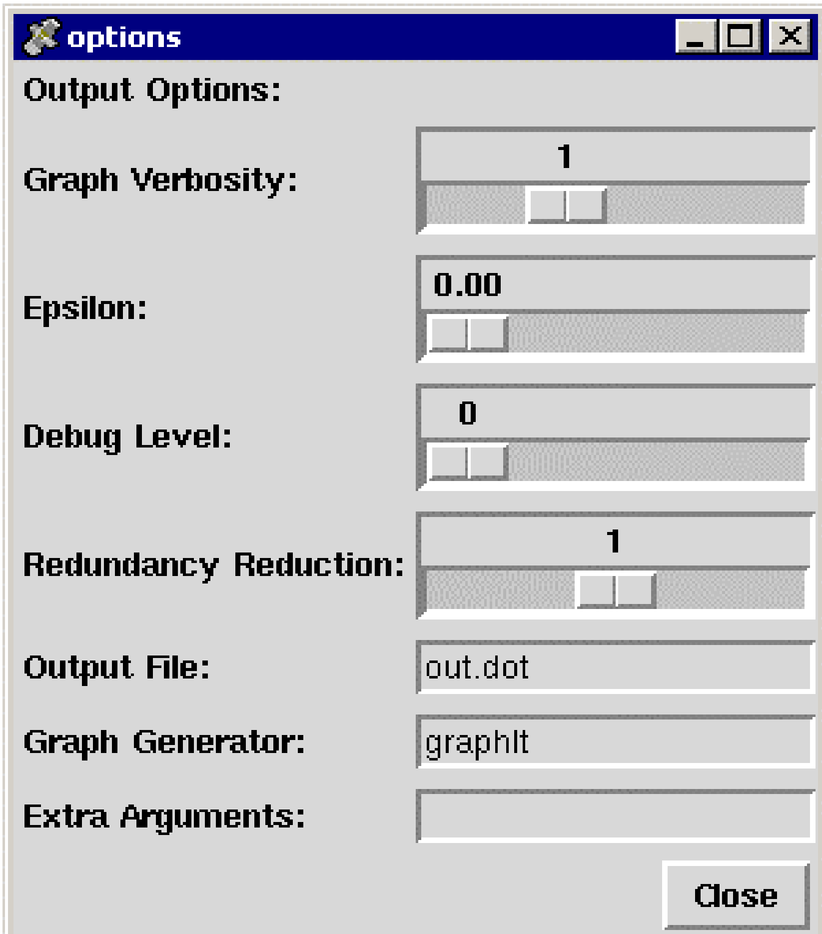
This is the main form for running the graph generator code. It includes menus for specifying the directories where the templates and configuration files are located, specifying run options, specifying a start node, and running the program.

Graph Generator



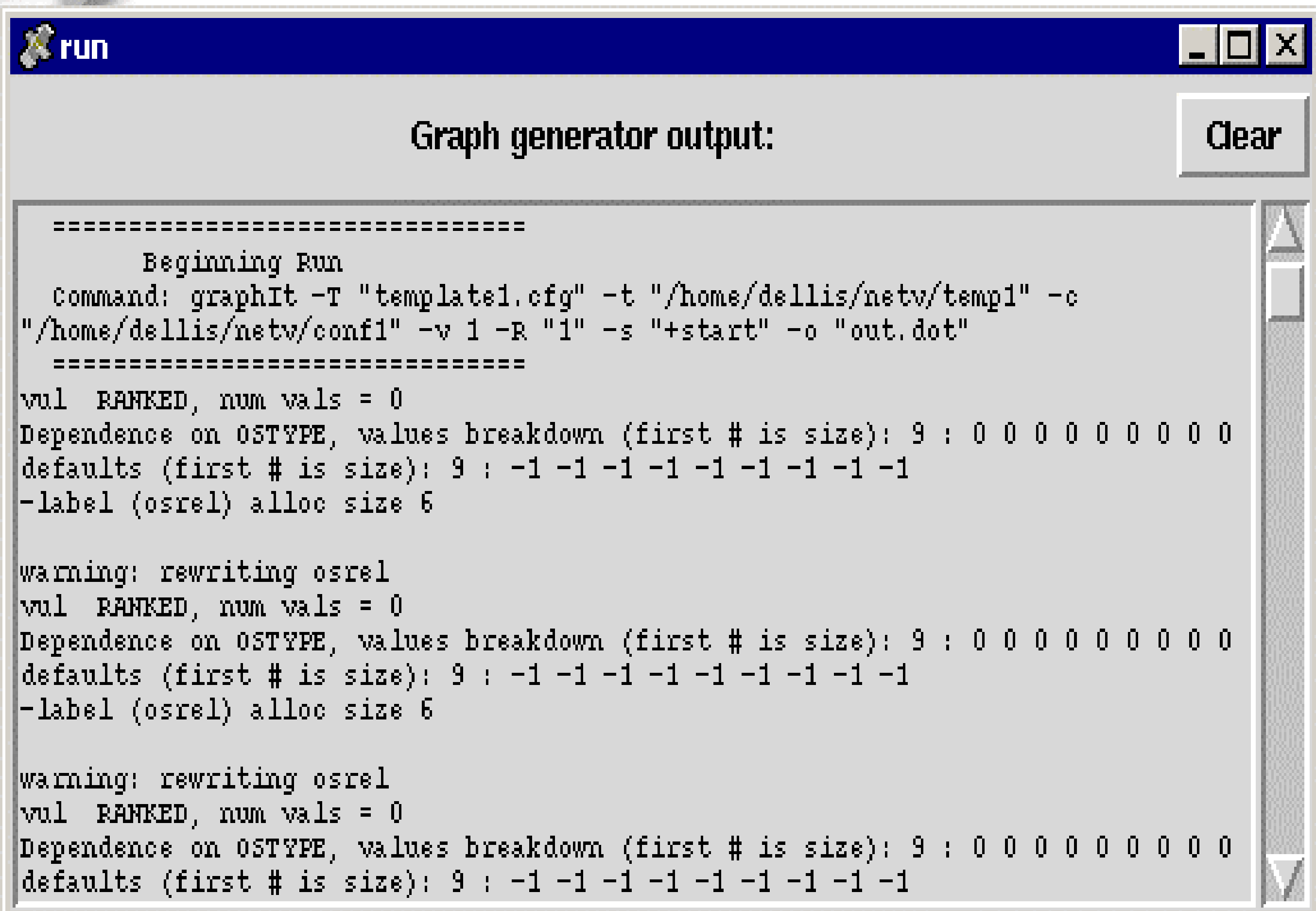
This form allows one to specify the location of the templates and configuration files

Graph Generator



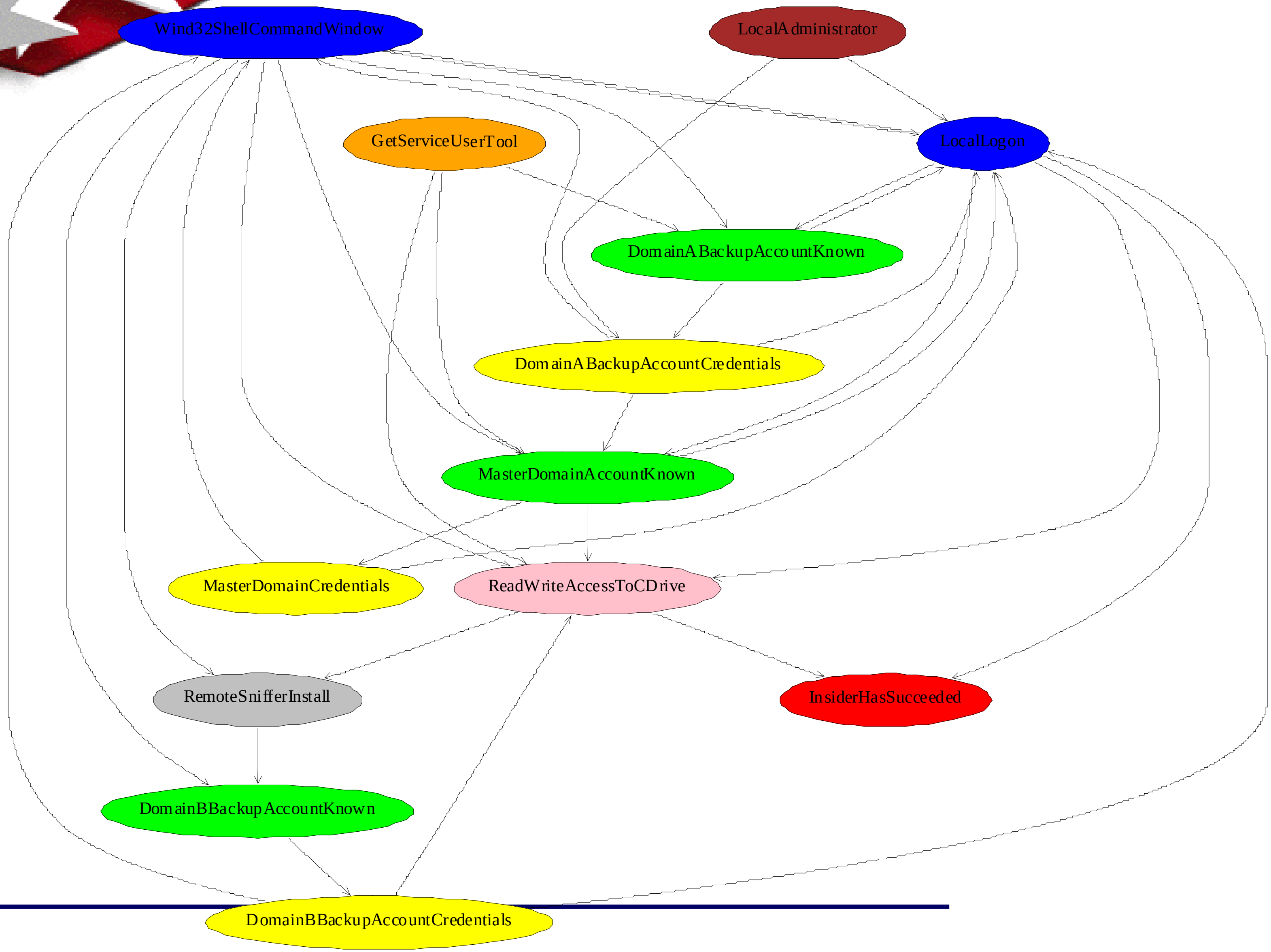
The form allows the user to specify various run options, such as graph verbosity (how much labeling is printed on the nodes and edges), epsilon (used in the shortest path algorithm), debugging level, name of the output file, etc.

Graph Generator

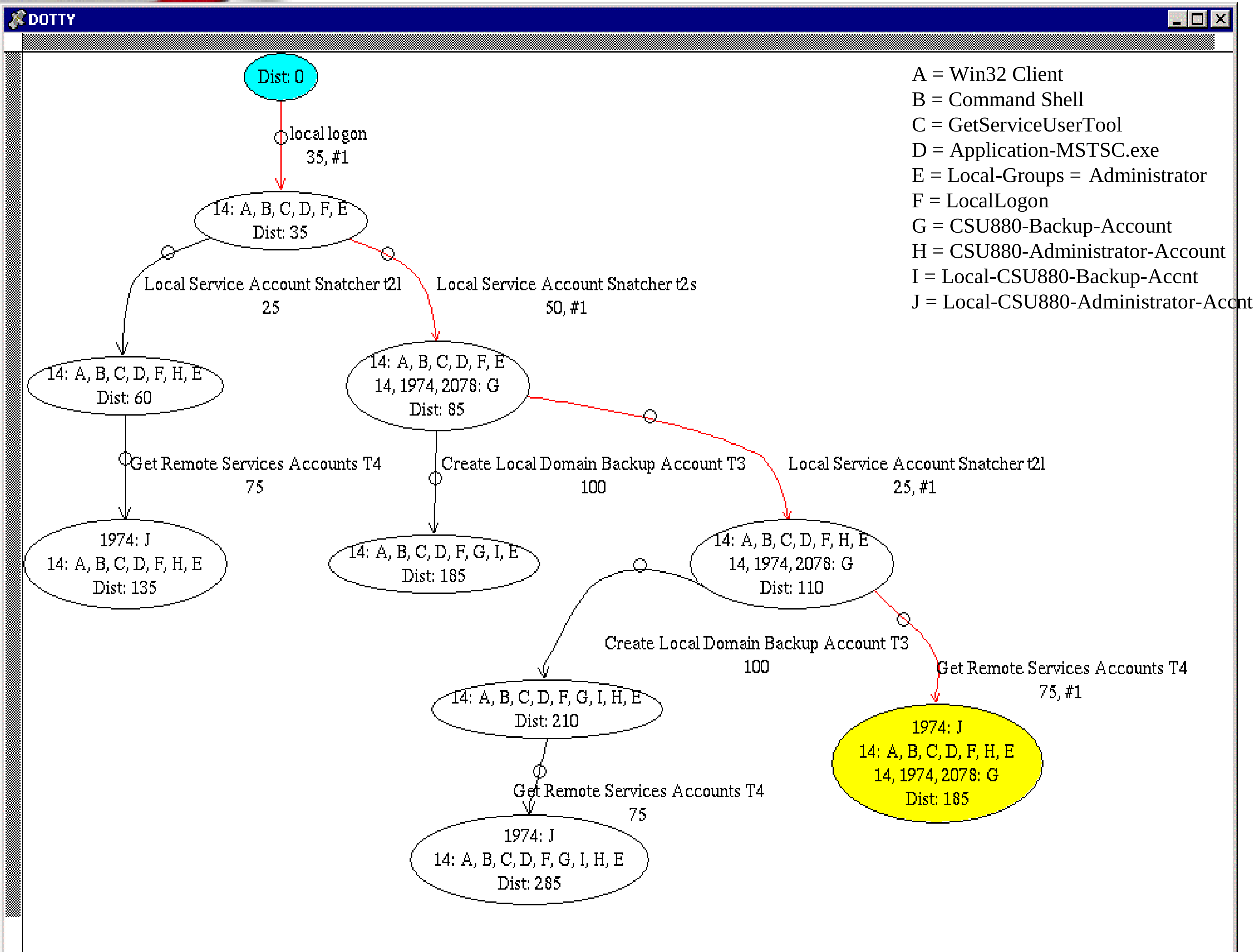


Example text output during an actual run

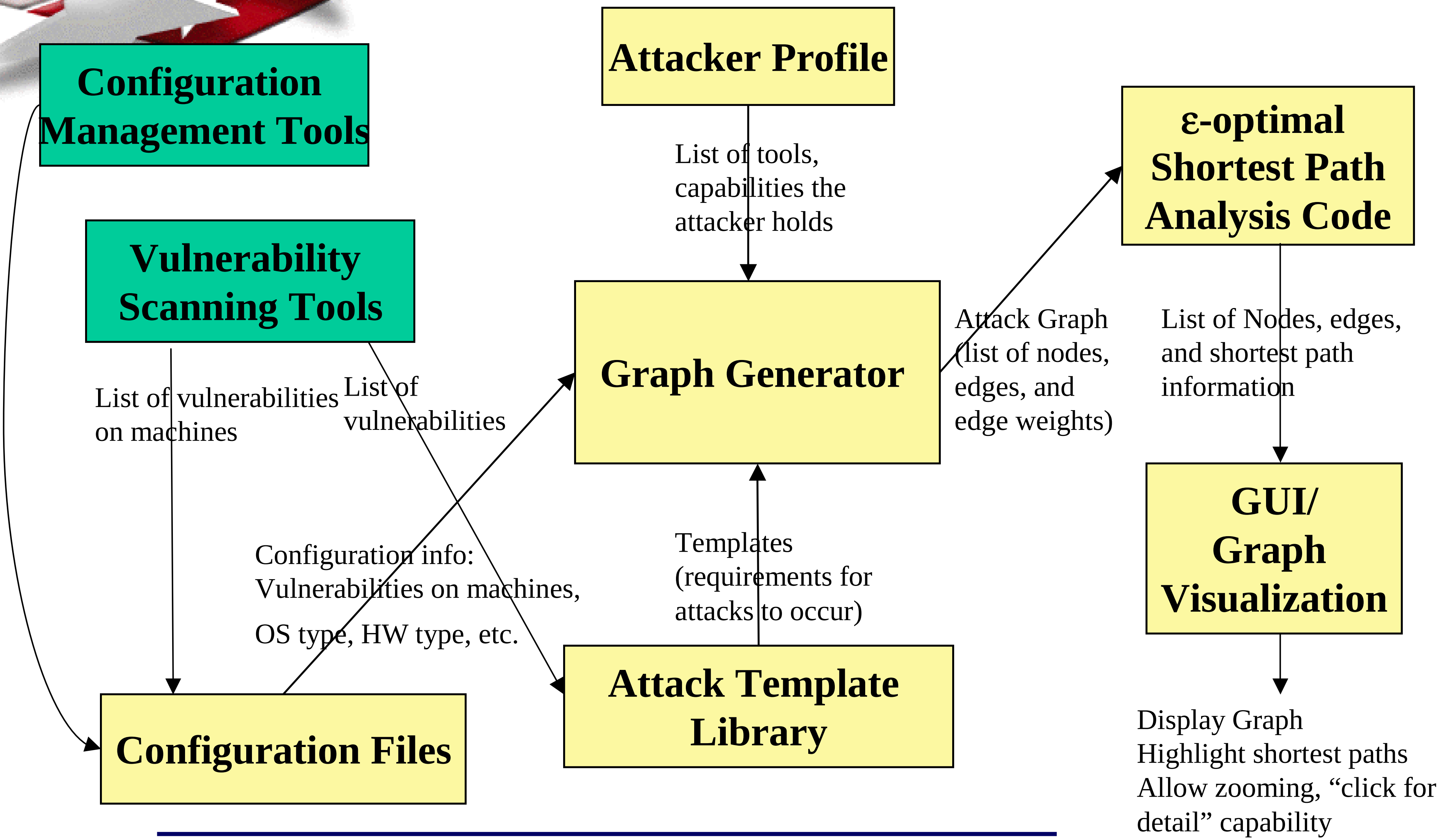
Ancestor Graph Example



Attack Graph Example



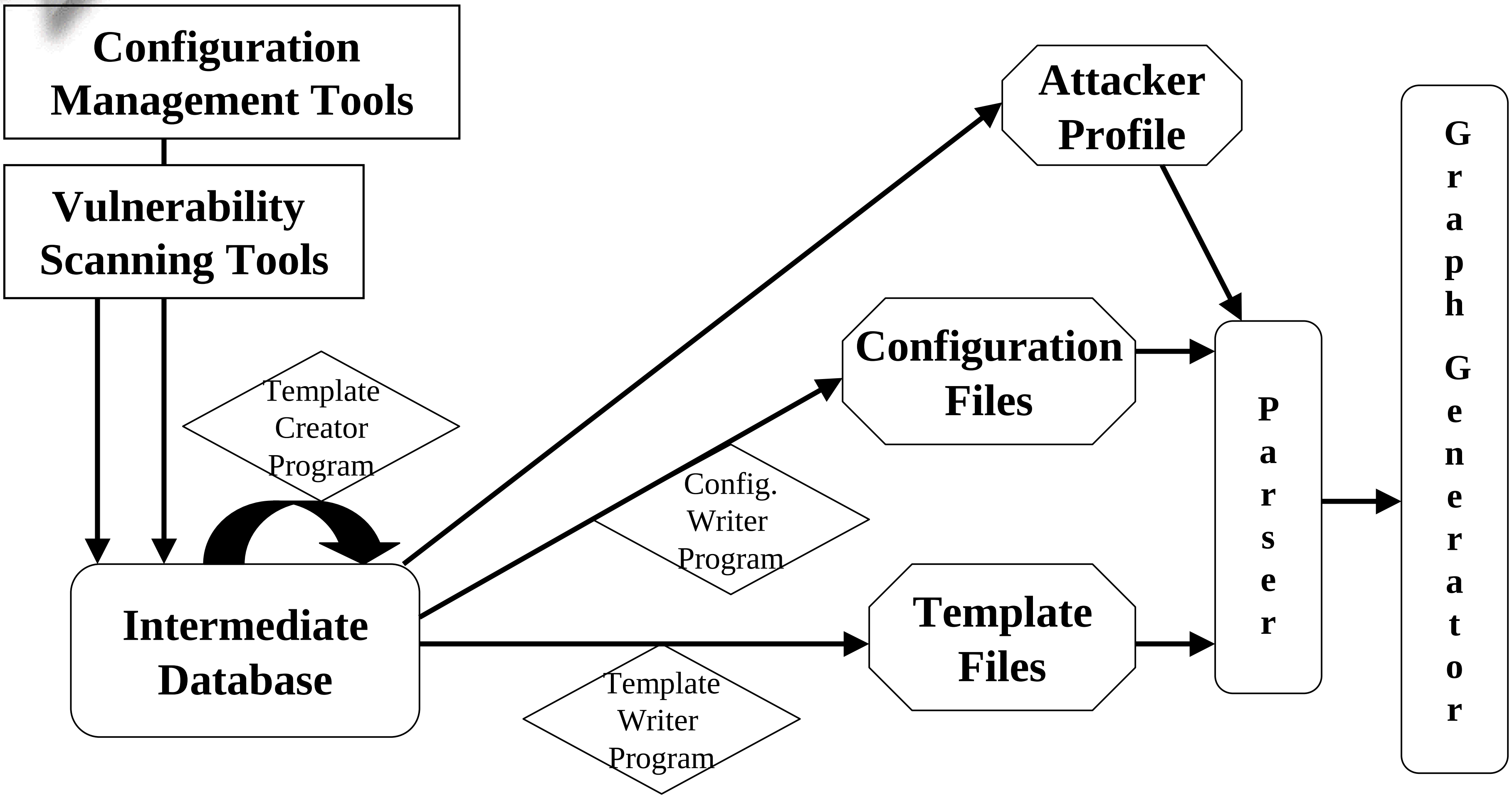
Functional Architecture



Current Status

- **Data Architecture**
  - We have designed an "intermediate" database that holds the necessary fields from commercial databases (e.g. ISS, Microsoft)
  - We have written queries to pull the data from the intermediate database to the C++ data structures for graph generation
  - Use of standardized terms in the templates and configuration data to ensure consistency for matching by the graph generator
  - Preprocess configuration data to only include attributes that are required by one of the templates
- **Scaling Issues**
  - Path redundancy elimination
  - Node redundancy elimination

Data Flow


Configuration Management Tools
Vulnerability Scanning Tools
Template Creator Program
Intermediate Database
Attacker Profile
Configuration Files
Config. Writer Program
Template Files
Template Writer Program
Parser
Graph Generator

Scaling

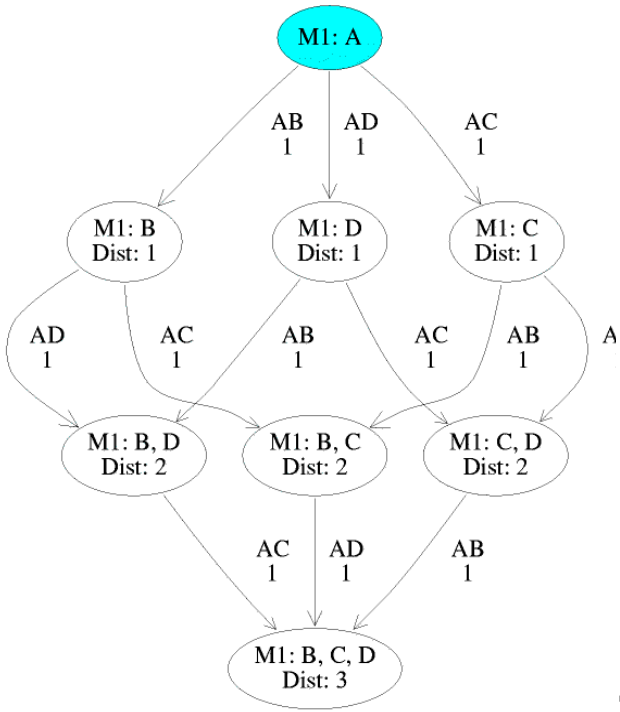
Redundant path elimination

- **2 vulnerabilities (A, B) are independent if A cannot be used directly or indirectly to acquire B and vice versa**
- **2 paths are redundant if they use the same set of templates and differ only in the order of acquisition of independent vulnerabilities**
- **We force an ordering or ranking amongst all independent vulnerabilities to eliminate redundant paths**

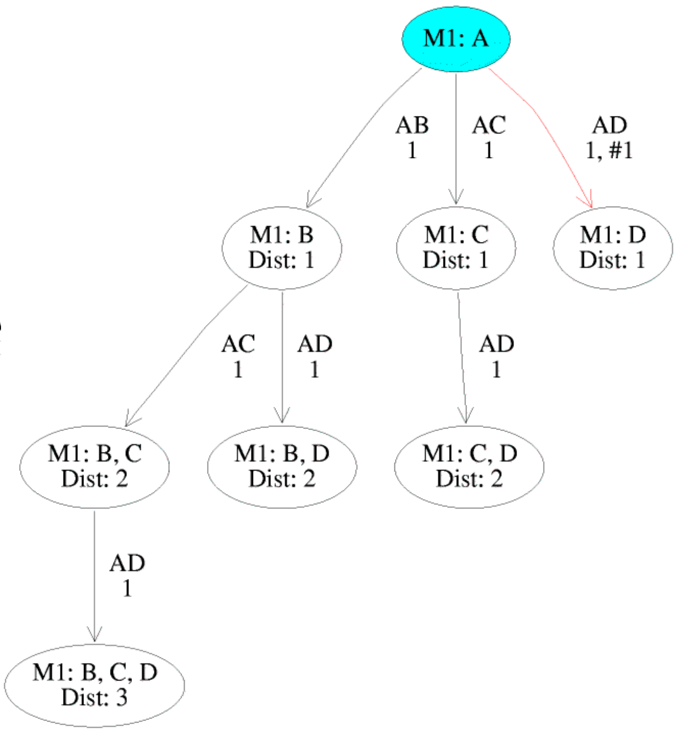
Redundant node elimination

- **In forward (exploratory) phase, we generate sets of independent attribute changes *only if* they lead *in combination* to new vulnerabilities**
- **Currently exploring algorithms for elimination of redundant nodes**

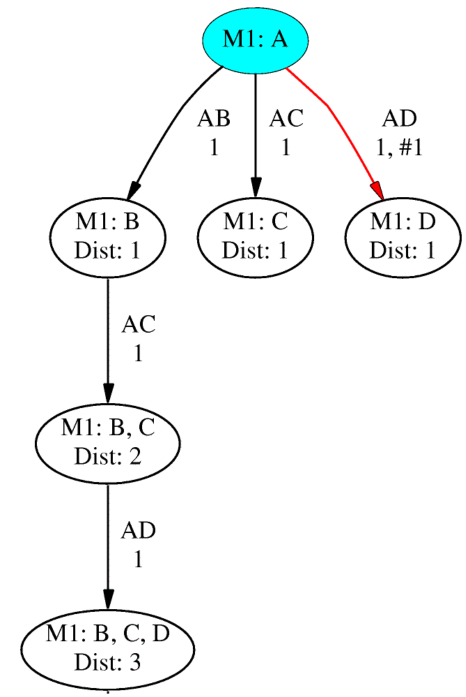
Redundancy Elimination



Graph with no redundancy elimination

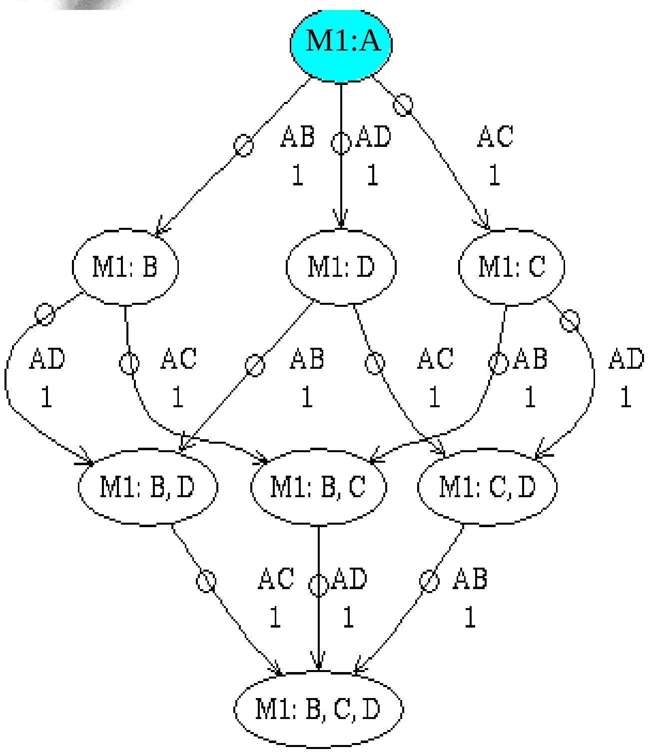


Graph with path redundancy elimination

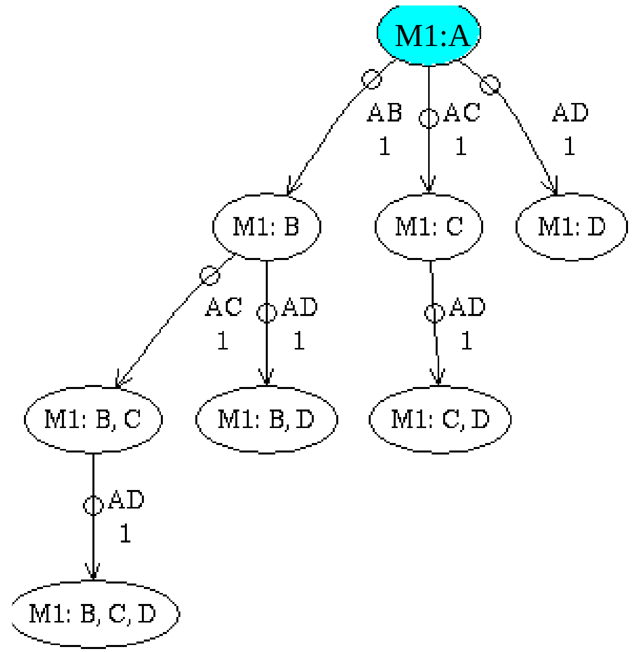


Graph with path and node redundancy elimination

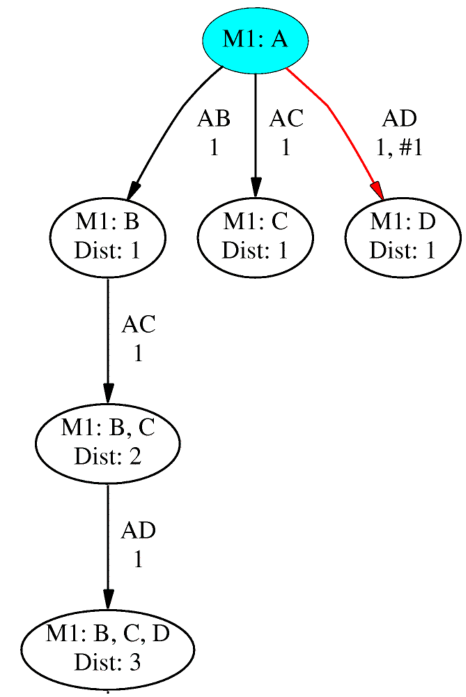
Redundancy Elimination



Graph with no redundancy elimination



Graph with path redundancy elimination



Graph with path and node redundancy elimination

Future of our tool

- Existing funding lasts through Dec. 01
- Looking for partners and funding sources to continue development of tool
- Potential uses:
  - Adversary modeling (e.g., red teams)
  - Network Design (security evaluation of design alternatives)
  - In conjunction with intrusion detection and sniffing devices
  - As a correlation tool to examine existing beliefs about network insecurity, correlate this with attack graph results